IN THE CLAIMS:

1. (Currently Amended) A method for certificate generation that enables efficient revocation of said certificate, comprising:

at a first node:

receiving a request to issue a certificate on behalf of a principal; and

forwarding said request to a second node, wherein said request includes a first identifier that identifies the first node; and

at the second node:

in response to receipt of the request, generating a certificate that includes said first identifier.

2. (Original) The method of claim 1 wherein said request further includes a second identifier that identifies a principal.

3. (Original) The method of claim 2 wherein said certificate further includes a public key associated with said principal, and said second identifier.

4. (Previously Presented) The method of claim 1 further including authenticating said certificate by said second node.

5. (Previously Presented) The method of claim 4 wherein authenticating said certificate comprises generating a certificate digitally signed by said second node.

6. (Previously Presented) The method of claim 5 wherein generating said certificate signed by said second node comprises generating a certificate digitally signed by said second node using a private key of a public private key pair associated with said second node.

7. (Original) The method of claim 1 wherein said certificate further includes a time stamp that identifies a time associated with the request.

8. (Previously Presented) The method of claim 1 further including authenticating said request by said first node.

9. (Previously Presented) The method of claim 8 wherein authenticating said request by said first node comprises digitally signing said request.

10. (Previously Presented) The method of claim 9 wherein digitally signing said request comprises the step of digitally signing said request using a private key of a public/private key pair associated with said first node.

11. (Original) The method of claim 1 wherein said certificate further includes a time stamp that is associated with a time and date when said request was received by said second node.

12. (Withdrawn) A method for determining whether access to a resource should be provided to a principal in response to a request for access to the resource by the principal comprising the steps of:

receiving said request for access to said resource from said principal at a server;

verifying the authenticity of said request using a key contained within a certificate associated with said principal;

determining whether a registration authority identifier within said certificate corresponds to a registration identifier contained on a certificate revocation list, wherein said registration authority identifier is associated with a registration authority that requested a certification authority to generate said certificate; and

providing an indication to said server that said certificate has been revoked and denying access of said principal to said resource in response to a determination that said registration authority identifier within said certificate corresponds to a registration authority identifier on said certificate revocation list.

13. (Withdrawn) The method of claim 12 wherein said determining step further comprises the step of determining whether a time stamp contained within said certificate that specifies a time of receipt of a request from said registration authority to the certification authority to generate the certificate corresponds to a period identified on said certificate revocation list during which the respective registration authority is indicated to be untrustworthy; and

said providing step comprises the step of providing said indication to said server that said certificate has been revoked and denying access of said principal to said resource in response to a determination that said registration authority identifier within said certificate corresponds to said registration authority identifier on said certificate revocation list and said time stamp within said certificate corresponds to a time within said period identified on said certificate revocation list during which said registration authority was indicated to be untrustworthy.

14. (Withdrawn) The method of claim 13 wherein said period has a beginning point and an assumed ending point, said beginning point being specified by a time value contained within said certificate revocation list and the assumed ending point corresponds to a present time value.

15. (Withdrawn) The method of claim 13 wherein said period has a beginning point and an ending point, said beginning point being specified by a first time value and the ending point corresponds to a second time value.

16. (Withdrawn) The method of claim 12 wherein said verifying and determining steps are performed by said server.

17. (Currently Amended) A certification authority comprising:

a memory containing a computer program for generating a certificate that enables efficient revocation of said certificate; and

a processor operative to execute said computer program, said computer program containing program code for:

receiving a request from a registration authority to issue a certificate on behalf of a principal; and

in response to receipt of said request, generating said certificate that includes at least a registration authority identifier associated with said registration authority.

18. (Original) The certification authority of claim 17 wherein said request to issue said certificate is an authenticated request and said computer program further includes program code for verifying said authenticated request.

19. (Previously Presented) The certification authority of claim 17 wherein said certificate generated by said computer program further includes a principal identifier associated with said principal and a key associated with said principal.

20. (Original) The certification authority of claim 17 wherein said computer program further includes program code for storing within said certificate a time stamp associated with a time when said certification authority received said request from said registration authority.

21. (Withdrawn) A system for determining whether access to a resource should be provided to a principal in response to a request for access to the resource by the principal comprising:

a first server operative to receive a request for access to said resource from said principal, said first server being operative to verify the authenticity of said request using a key contained within said certificate associated with said principal, wherein said certificate includes at least a registration authority identifier associated with a registration authority that issued a request to a certification authority to issue said certificate;

a second server containing a certificate revocation list, wherein said certificate revocation list includes said registration authority identifier in the event the associated registration authority has been determined to be untrustworthy, said second server being operative in response to a certificate revocation inquiry request to ascertain whether said certificate revocation list contains a registration authority identifier that corresponds to said registration authority identifier within said certificate; and

said second server being further operative to provide an indication to said first server that said certificate has been revoked in the event said certificate revocation list contains said registration authority identifier that corresponds to said registration authority identifier within said certificate.

22. (Withdrawn) The system of claim 21 wherein said first and second server comprise a single server.

23. (Withdrawn) The system of claim 21 wherein said first server is further operative in response to receipt of said indication that said certificate has been revoked to deny said principal access to said requested resource.

24. (Withdrawn) The system of claim 21 wherein said certificate further includes a time stamp associated with a time when said certification authority received from said registration authority said request to issue said certificate on behalf of said principal; and

wherein said certificate revocation list includes said registration authority identifier in the event the associated registration authority has been determined to be untrustworthy and at least one value defining a time interval during which said registration authority is deemed to be untrustworthy,

said second server being operative in response to a certificate revocation inquiry request to provide a revocation inquiry request to provide a revocation indication if said certificate revocation list contains a registration authority identifier that corresponds to said registration authority identifier within said certificate and a time stamp associated with said registration authority identifier that is within said interval.

25. (Withdrawn) The system of claim 23 wherein said second server comprises a revocation server.

26. (Withdrawn) The system of claim 25 wherein said revocation server is further operative in response to said revocation indication to forward a certificate revocation message to said first server that indicates that said certificate has been revoked.

27. (Withdrawn) The system of claim 26 wherein said first server is operative in response to said certificate revocation message to deny said principal access to said requested resource.

28. (Currently Amended) A computer program product including a computer readable medium, said computer readable medium having a computer program stored thereon for generating a certificate that enables efficient revocation of said certificate, said computer program being executable by a processor and comprising:

program code for receiving a request from a registration authority to issue a certificate on behalf of a principal; and

program code operative in response to recognition of said request, for generating by a certification authority a certificate authenticated by said certification authority wherein said certificate includes at least a principal identifier associated with said principal, a key associated with said principal for use in authenticating messages generated by said principal, and a registration identifier associated with said registration authority.

29. (Original) The computer program product of claim 28 wherein said program code for generating said certificate is further operative to include within said certificate a time stamp associated with a time or receipt by said certification authority of said request from said registration authority of said request to issue said certificate.

30. (Currently Amended) A computer data signal, said computer data signal including a computer program for use in generating a certificate that enables efficient revocation of said certificate, said computer program comprising:

program code for receiving a request from a registration authority to issue a certificate on behalf of a principal; and

program code operative in response to recognition of said request, for generating by a certification authority a certificate authenticated by said certification authority wherein said certificate includes at least a principal identifier associated with said principal, a key associated with said principal for use in authenticating messages generated by said principal, and a registration identifier associated with said registration authority.

31. (Original) The computer data signal of claim 30 wherein said program code for generating said certificate is operative to include within said certificate a time stamp associated with a time of receipt by said certification authority from said registration authority of said request to issue said certificate.

32. (Original) The computer data signal of claim 30 wherein said computer program further includes program code for publishing said certificate.

33. (Previously Presented) The computer data signal of claim 32 wherein said program code for publishing said certificate includes program code for forwarding said certificate to a directory server.

34. (Currently Amended) An apparatus for generating a certificate in a computer network, wherein said generating of said certificate enables efficient revocation of said certificate, the apparatus comprising:

means operative in response to receipt of a request from a first node coupled to said computer network at a second node coupled to said computer network for generating at said second node a certificate on behalf of a principal that includes a first node identifier associated with said first node.

35. (Currently Amended) The apparatus of claim 34 wherein said request was initiated by ~~a~~ said principal and said request includes a principal identifier associated with said principal and said certificate further includes said principal identifier and a public key associated with said principal.

36. (Original) The apparatus of claim 34 wherein said certificate is authenticated by said second node.

37. (Previously Presented) The apparatus of claim 34 further including means for comparing said first node identifier to a node identifier associated with an untrustworthy node on said network that is included within a certificate revocation list and providing an indication that said certificate is untrustworthy in the event said first node identifier matches said untrustworthy node identifier.